IN THE CLAIMS

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims

1. (Currently Amended) A method for providing a secure computing environment, comprising:

providing a portable encryption control device~~, the encryption control device being in communication with a computer and a smart card~~;

attaching the portable encryption control device to a computing device;

triggering a bus reset on the computer in response to attaching the portable encryption control device;

enabling a user to control and customize the portable encryption control device features through a system tray utility program;

authenticating ~~a~~ the user as a valid owner of ~~the~~ a smart card;

initializing the encryption control device through a challenge/response protocol with the smart card if the valid owner is authenticated; ~~and~~

activating an encryption/decryption engine of the encryption control device to enable access to data in a secure computing environment if the challenge response protocol is executed successfully;

enabling the user to add a secondary user to the smart card; and

setting the secondary user's level of access to the portable encryption control device.

2. (currently amended) The method as recited in claim 1, wherein the authenticating ~~a~~ the user as a valid owner of the smart card includes providing a personal identification number.

3. (currently amended) The method as recited in claim 1, wherein the authenticating ~~a~~ the user as a valid owner of the smart card includes providing a biometric identifier.

4. (Original) The method as recited in claim 1, wherein the challenge/response protocol includes an exchange of private and public keys between the encryption control device and a smart card.

5. (Original) The method as recited in claim 1, wherein a biometric scanner is employed for authenticating a user.

6. (Original) The method as recited in claim 1, further including,

monitoring for continued presence of the valid owner; and

locking the encryption control device if the valid owner is not detected.

7. (Original) The method as recited in claim 1, wherein the smart card stores the user's personal data.

8. (Original) The method as recited in claim 1, wherein a personal identification number is used to authenticate a user.

9. (Original) The method as recited in claim 1, further including,

providing control switches for bypassing the encryption control device.

10. (Currently Amended) A method for activating an encryption control device that is in communication with a computer for providing a secure computing environment for a user, comprising:

providing a card for insertion into a card reader of the portable encryption control device, the card being configured to receive and pass data;

attaching the portable encryption device to the computer;

triggering a bus reset on the computer in response to attaching the portable encryption control device;

enabling a user to control and customize the portable encryption control device features through a system tray utility program, the enabling including,

tracking unauthorized attempts made to access the portable encryption control device, and

allowing for remote shutdown of the portable encryption control device;

receiving a biometric identifier from the user, the biometric identifier enabling validation of the user as the authorized owner of the card;

running a challenge/response protocol between the encryption control device and the inserted card, the challenge/response protocol establishing that the inserted card and the encryption control device are compatible; and

activating an encryption/decryption engine of the encryption control device to create a secure computing environment if the user is validated as the authorized owner of the card and challenge response protocol is successfully executed;

enabling the user to add a secondary user to the smart card; and

setting the secondary user's level of access to the portable encryption control device.

11. (Canceled)

12. (Original) The method as recited in claim 10, wherein the encryption engine executes RSA public-key cryptosystem.

13. (Canceled)

14. (Original) The method as recited in claim 10, wherein the data are public and private keys.

15. (Canceled)

16. (Currently Amended) The method as recited in claim 10, wherein execution of the challenge/response protocol establishes a secure path between the encryption control device and the inserted card, the secure path allowing for configuration and biometric data from the encryption control device to be transferred to the inserted card and allowing data from the inserted card to be downloaded to the encryption control device.

17. (Currently Amended) A method for operating a computer in a secure mode, comprising:

~~providing~~ attaching ~~an~~ a portable encryption control device~~, the encryption control device~~ (ECD) ~~being in communication with the computer and a smart card, the encryption control device storing a biometric identifier of a user~~ to the computer;

triggering a bus reset on the computer in response to attaching the portable encryption control device;

enabling a user to control and customize the portable encryption control device features through a system tray utility program;

authenticating the user as a valid owner of the smart card, the authenticating further including,

receiving a biometric identifier from the user, and

comparing the received biometric indicator with the stored biometric indicator for a match; ~~and~~

activating an encryption/decryption engine of the encryption control device to create a secure operating mode if the user is authenticated;

enabling the user to add a secondary user to the smart card upon authentication; and

setting the secondary user's level of access to the portable encryption control device.

18. (Currently Amended) The method as recited in claim ~~16~~ 17, wherein the ECD includes a storage medium for storing encrypted data.

19. (Currently Amended) The method as recited in claim ~~16~~ 17, wherein encrypted data is stored on a virtual drive of the computer.

20. (Currently Amended) The method as recited in claim ~~16~~ 17, further including;

allowing the user to transfer unencrypted data from a non-secure storage drive to a secure storage drive, the secure storage drive storing data in an encrypted format.

21. (New) The method as recited in claim 1, wherein enabling a user to control and customize the portable encryption control device features through a system tray utility program includes,

tracking unauthorized attempts made to access the portable encryption control device, and

allowing for a remote shutdown of the portable encryption control device.

22. (New) The method as recited in claim 17, wherein enabling a user to control and customize the portable encryption control device features through a system tray utility program includes,

tracking unauthorized attempts made to access the portable encryption control device, and

allowing for a remote shutdown of the portable encryption control device.